

OPES Treatment of IAB Considerations
draft-ietf-opes-iab-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 11, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

IETF Internet Architecture Board (IAB) expressed nine architecture-level considerations when Open Pluggable Edge Services (OPES) working group was being chartered at the IETF. The working group was chartered under the condition that IAB considerations were addressed by the group. This document describes how OPES addresses those considerations.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Consideration (2.1) One-party consent	5
4.	Consideration (2.2) IP-layer communications	6
5.	Notification Considerations	8
5.1	Consideration (3.1) Notification	9
5.2	Consideration (3.2) Notification	10
5.3	Consideration (3.3) Non-blocking	11
6.	Consideration (4.1) URI resolution	12
7.	Consideration (4.2) Reference validity	13
8.	Consideration (4.3) Addressing extensions	14
9.	Consideration (5.1) Privacy	15
10.	Security Considerations	16
11.	Compliance	17
12.	To-do	18
A.	Change Log	19
	Normative References	20
	Informative References	21
	Authors' Addresses	21
	Intellectual Property and Copyright Statements	22

1. Introduction

The Open Pluggable Edge Services (OPES) architecture [[I-D.ietf-opes-architecture](#)], enables cooperative application services (OPES services) between a data provider, a data consumer, and zero or more OPES processors. The application services under consideration analyze and possibly transform application-level messages exchanged between the data provider and the data consumer.

Following controversy related to chartering OPES, IAB made recommendations on issues that OPES solutions should be required to address. These recommendations were formulated in the form of specific IAB considerations [[RFC3238](#)]. IAB emphasized that its considerations did not recommend specific solutions and did not mandate specific functional requirements. Addressing an IAB consideration may involve showing appropriate protocol mechanisms or demonstrating that the issue does not apply.

The primary goal of this document is to show that all IAB considerations are addressed by OPES, to the extent those considerations can be addressed by an IETF working group. We also explicitly document limitations of our abilities to address certain aspects of IAB considerations.

There are nine IAB considerations [[RFC3238](#)] that OPES has to address. In the core of this document are the corresponding nine "Consideration" sections. For each IAB consideration, its section contains general discussion as well as references to specific OPES mechanisms relevant to the consideration.

2. Terminology

This document does not introduce any new terminology but uses terminology from other OPES documents it quotes.

3. Consideration (2.1) One-party consent

"An OPES framework standardized in the IETF must require that the use of any OPES service be explicitly authorized by one of the application-layer end-hosts (that is, either the content provider or the client)."[[RFC3238](#)]

OPES architecture requires that "OPES processors MUST be consented to by either the data consumer or data provider application" [[I-D.ietf-opes-architecture](#)]. The requirement alone cannot prevent consent-less introduction of OPES processors, of course. OPES enables concerned parties to detect unwanted OPES processors by examining OPES traces and by checking content signatures.

Tracing is a weak but cheap mechanism that is unable to detect processors incompilant with OPES specifications on tracing and operating in stealth mode. Content signatures is a strong but expensive mechanism that can detect any modifications of signed content provided the content provider is willing to sign the data and the client is willing to either check the signature or relay received content to content provider for signature verification.

OPES adaptations include copying and other forms of non-modifying access to content. These kinds of adaptations cannot be detected by the above mentioned mechanisms. Thus, "passive" unwanted OPES processors cannot be detected. If presence of such processors is a concern, content encryption can be used. See privacy consideration for more details.

4. Consideration (2.2) IP-layer communications

"For an OPES framework standardized in the IETF, the OPES intermediary must be explicitly addressed at the IP layer by the end user."[\[RFC3238\]](#)

OPES architecture requires that "OPES processors MUST be addressable at the IP layer by the end user (data consumer application)" [\[I-D.ietf-opes-architecture\]](#). Two caveats are related to this requirement. First, addressing the first OPES processor in a chain of processors is sufficient. That is, a chain of OPES processors is viewed as a single OPES processor at the address of the first chain element. (XXX: should we move these caveats into a separate section? they seem to affect many considerations; one the other hand, it is probably the job of the architecture draft to define these things so that we can refer to them from here.)

The second caveat is more controversial. Only a very limited subset of OPES intermediaries are subject to the above requirements. The situation is examined below, by considering content provider and end user sides of the architecture.

OPES processors that operate under content provider consent may not be subject to the above consideration and requirement (XXX the architecture draft does not reflect this). It is irrational to expect a content provider to provide access to internal hosts participating in content generation, whether OPES processors are involved or not. Moreover, providing such access would serve little practical purpose because internal OPES processors are not likely to be able to answer any end user queries, being completely out of content generation context. For example, an OPES processor adding customer-specific information to XML pages may not understand or be aware of any final HTML content that the end user receives and may not be able to map end user request to any internal user identification.

OPES processors that operate under end user consent may not be subject to the above consideration and requirement (XXX the architecture draft does not reflect this). It is irrational to expect a client-side ISP to provide access to internal hosts participating in content processing, whether OPES processors are involved or not. Moreover providing such access would serve little practical purpose because internal OPES processors are not likely to be able to answer any end user queries, being completely out of content processing context. For example, an OPES processor making a client-authorized XML content translation may not understand or be aware of any final HTML content that the end user receives and may not be able to map end user request to any internal user identification.

IAB consideration 2.2 apparently was not meant to apply to "internal" OPES intermediaries. It may be better interpreted as "If the first intermediary on end user's message processing path is an OPES intermediary, that intermediary must be explicitly addressed at the IP layer by the end user". In other words, the end user is assured that the first intermediary that touches her request is explicitly addressed if it is an OPES intermediary.

(XXX: should we add a picture showing internal and external OPES intermediaries?)

5. Notification Considerations

This section discusses how OPES framework addresses IAB Notification concerns 3.1 and 3.2. OPES framework concentrates on tracing rather than notification. The tracing specification [XXX] defines "OPES trace" as "application message information about OPES entities that adapted that message" and "OPES tracing" as "the process of including, manipulating, and interpreting an OPES trace" (XXX: keep these in sync). Thus, OPES trace follows the application message it traces. It notifies the recipient of the message of what has happened to that message. Traces are implemented as extensions of application protocols being adapted and traced.

As opposed to an OPES trace, provider notification (as implied by IAB) notifies the sender of the message of what had happened to the message after the message left the sender. Thus, notifications propagate in the opposite direction of traces. Supporting notifications directly would require a new protocol. Figure XXX illustrates the differences between a trace and notification from a single application message point of view.

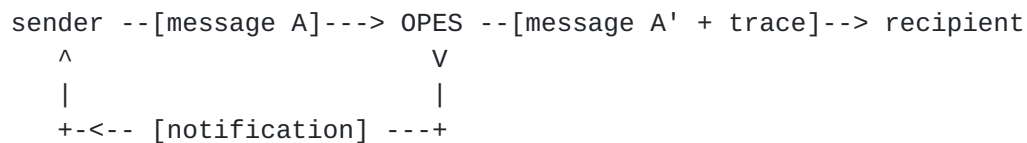


Figure 1

Since notifications cannot be piggy-backed to application messages, they create new messages and may at least double the number of messages the sender has to process (more if several intermediaries on the message path emit notifications). Moreover, a notification message may refer to some sender state that has to be kept around until notification is received, increasing performance overhead of notifications. These concerns call for optional notification, with a special protocol to enable notifications when needed.

The level of available details in notifications versus provider interest in supporting notification is another concern. Experience shows that content providers often require very detailed information about user actions to be interested in notifications at all. For example, Hit Metering protocol [XXX] has been designed to supply content providers with proxy cache hit counts, in an effort to reduce cache busting behavior which was caused by content providers desire to get accurate site "access counts". However, the Hit Metering protocol is currently not widely deployed because the protocol does not supply content providers with information such as client IP addresses, browser versions, or cookies.

The Hit Metering experience is relevant because Hit Metering protocol was designed to do for HTTP caching intermediaries what OPES notifications are meant to do for OPES intermediaries. Performance requirements call for state reduction via aggregation of notifications while provider preferences call for state preservation or duplication. Achieving the right balance when two sides belong to different organizations and have different optimization priorities is probably impossible in general.

Thus, instead of explicitly supporting notifications on a protocol level, OPES concentrates on tracing facilities and supports notifications indirectly, using those tracing facilities. In other words, the IAB choice of "Notification" label is interpreted as "Notification assistance" (i.e. making notifications meaningful) and is not interpreted as a "Notification protocol".

5.1 Consideration (3.1) Notification

"The overall OPES framework needs to assist content providers in detecting and responding to client-centric actions by OPES intermediaries that are deemed inappropriate by the content provider."[\[RFC3238\]](#)

OPES tracing mechanisms assist content providers in detecting client-centric actions by OPES intermediaries. Specifically, a compliant OPES intermediary or system notifies a content provider of its presence by including its tracing information in the application protocol requests. An OPES intermediary **MUST** leave its trace (XXX quote tracing draft). Detection assistance has its limitations. Some OPES intermediaries may work exclusively on responses and may not have a chance to trace the request. Moreover, some application protocols may not have explicit requests (e.g., a content push service).

OPES tracing mechanisms assist content providers in responding to client-centric actions by OPES intermediaries. Specifically, OPES traces **MUST** include identification of OPES systems and **SHOULD** include a list of adaptation actions performed on provider's content. This tracing information may be included in the application request. Usually, however, this information will be included in the application response, an adapted version of which does not reach the content provider. If OPES end points cooperate, then notification can be assisted with traces. Content providers that suspect or experience difficulties can do any of the following:

Check whether requests they receive pass through OPES intermediaries. Presence of OPES tracing info will determine that. This check is only possible for request/response protocols. For

other protocols (e.g., broadcast or push), the provider would have to assume that OPES intermediaries are involved until proven otherwise.

If OPES intermediaries are suspected, request OPES traces from potentially affected user(s). The trace will be a part of the application message received by the user software. If users cooperate, the provider(s) have all the information they need. If users do not cooperate, the provider(s) cannot do much about it (they might be able to deny service to uncooperative users in some cases).

Some traces may indicate that more information is available by accessing certain resources on the specified OPES intermediary or elsewhere. Content providers may query for more information in that case.

If everything else fails, providers can enforce no-adaptation policy using appropriate OPES bypass mechanisms and/or end-to-end encryption mechanisms.

OPES detection and response assistance is limited to application protocols with support for tracing extensions. For example, HTTP [[RFC2616](#)] has such support while DNS over UDP does not.

(XXX: should we prohibit adaptation of application protocols that do not allow for tracing?)

[5.2](#) Consideration (3.2) Notification

"The overall OPES framework should assist end users in detecting the behavior of OPES intermediaries, potentially allowing them to identify imperfect or compromised intermediaries."[\[RFC3238\]](#)

OPES tracing mechanisms assist end users in detecting OPES intermediaries. Specifically, a compliant OPES intermediary or system notifies an end user of its presence by including its tracing information in the application protocol messages sent to the client. An OPES intermediary **MUST** leave its trace (XXX quote tracing draft). Detection assistance has its limitations. Some OPES intermediaries may work exclusively on requests and may not have a chance to trace the response. Moreover, some application protocols may not have explicit responses (e.g., event logging service).

OPES detection assistance is limited to application protocols with support for tracing extensions. For example, HTTP [[RFC2616](#)] has such support while DNS over UDP does not.

(XXX: should we prohibit adaptation of application protocols that do not allow for tracing?)

5.3 Consideration (3.3) Non-blocking

"If there exists a "non-OPES" version of content available from the content provider, the OPES architecture must not prevent users from retrieving this "non-OPES" version from the content provider."[\[RFC3238\]](#)

OPES intermediaries MUST support a bypass feature (XXX quote bypass draft). If an application message includes bypass instructions, the matching OPES intermediary will not process the message. Bypass may generate content errors since some OPES services may be essential. (Should there be a way to bypass non-essential services only?)

Bypass support has limitations similar to the two notification-related considerations above.

6. Consideration (4.1) URI resolution

"OPES documentation must be clear in describing these services as being applied to the result of URI resolution, not as URI resolution itself."[\[RFC3238\]](#)

"OPES Scenarios and Use Cases" specification
[\[I-D.ietf-opes-scenarios\]](#) documents content adaptations that are in scope of the OPES framework (XXX provide a quote). These adaptations do not include URI resolution (XXX check). In some environments, it is technically possible to adapt URIs (and other kinds of identifiers or addresses) using documented OPES mechanisms.

7. Consideration (4.2) Reference validity

"All proposed services must define their impact on inter- and intra-document reference validity."[\[RFC3238\]](#)

OPES working group does not propose adaptation services. However, OPES tracing requirements include identification of OPES intermediaries and services (for details, see "Notification" consideration sections in this document). It is required that provided identification can be used to locate information about the OPES intermediaries, including the description of impact on reference validity (XXX quote tracing draft).

8. Consideration (4.3) Addressing extensions

"Any services that cannot be achieved while respecting the above two considerations may be reviewed as potential requirements for Internet application addressing architecture extensions, but must not be undertaken as ad hoc fixes."[[RFC3238](#)]

OPES framework does not contain ad hoc services. This and other OPES documents should be sufficient to inform service creators of IAB considerations. If a service does URI resolution or silently affects document reference validity, the authors are requested to review service impact on Internet application addressing architecture and work within IETF on potential extension requirements.

9. Consideration (5.1) Privacy

"The overall OPES framework must provide for mechanisms for end users to determine the privacy policies of OPES intermediaries." [[RFC3238](#)]

OPES tracing mechanisms allow end users to identify OPES intermediaries (for details, see "Notification" consideration sections in this document). It is required that provided identification can be used to locate information about the OPES intermediaries, including their privacy policies.

The terms "privacy" and "privacy policy" are not defined in this context (by IAB or OPES working group). OPES tracing mechanisms allow end users and content providers to identify OPES intermediaries. It is believed that once an intermediary is identified, it would be possible to locate relevant information about that intermediary, including information relevant to requesters perception of privacy policy or reference validity. (XXX: should we move this paragraph into a separate section and expand it? one the other hand, it is probably the job of the architecture draft to define these things so that we can refer to them from here.)

10. Security Considerations

XXX.

11. Compliance

This document may be perceived as a proof of OPES compliance with IAB implied recommendations. However, this document does not introduce any compliance subjects. Compliance of OPES implementations is defined in other OPES documents discussed above.

12. To-do

security section: Does this document have any original security matters worth documenting?

normative IDs: To be normative, OPES Internet-Drafts must be replaced with corresponding RFCs when the latter are published.

architecture draft: Should architecture draft talk about external/internal OPES intermediaries and about privacy policies? Should this document be limited to a compilation of references from other OPES drafts, or should we introduce/discuss new concepts here?

[Appendix A](#). Change Log

Internal WG revision control ID: \$Id: iab-cons.xml,v 1.13 2003/06/12
15:38:48 rousskov Exp \$

head-sid9

- * Polished to meet new xml2rfc sctrict requirements.

head-sid8

- * Added unpolished meat for all nine considerations.
- * Added Abbie Barbir as an author.

head-sid7

- * Initial revision

Normative References

- [I-D.ietf-opes-architecture]
Barbir, A., "An Architecture for Open Pluggable Edge Services (OPES)", [draft-ietf-opes-architecture-04](#) (work in progress), December 2002.
- [I-D.ietf-opes-scenarios]
Barbir, A., "OPES Use Cases and Deployment Scenarios", [draft-ietf-opes-scenarios-01](#) (work in progress), August 2002.
- [RFC3238] Floyd, S. and L. Daigle, "IAB Architectural and Policy Considerations for Open Pluggable Edge Services", [RFC 3238](#), January 2002.

Informative References

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Nielsen, H.,
Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext
Transfer Protocol -- HTTP/1.1", [RFC 2616](#), June 1999.

Authors' Addresses

Abbie Barbir
Nortel Networks
3500 Carling Avenue
Nepean, Ontario
CA

Phone: +1 613 763 5229
EMail: abbieb@nortelnetworks.com

Alex Rousskov
The Measurement Factory

EMail: rousskov@measurement-factory.com
URI: <http://www.measurement-factory.com/>

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the
Internet Society.